

JOHN FRIEDLANDER and HENRYK IWANIEC

Sums over vanishing determinants

Abstract. In analytic number theory one frequently needs to estimate various bilinear sums, in particular exponentials with Kloosterman type fractions. Here, we establish bounds which go beyond the straight-forward approach.

Keywords. Gaussian integers, large sieve inequality.

Mathematics Subject Classification: 11N25, 11N56.

Contents

1	Introduction	49
2	A few observations about other restricted sums	52
3	Statement of the theorem	53
4	First estimation of $S(Q, X)$	54
5	Second estimation of $S(Q, X)$	57
6	Leapfrog and completing the proof	60

1 - Introduction

Among the simplest determinants are those which appear in the resolution of systems of two linear equations:

$$(1.1) \quad \begin{aligned} u_1x + v_1y &= a, \\ u_2x + v_2y &= b. \end{aligned}$$

Received: February 3, 2020; accepted in revised form: March 19, 2020.

We are interested in the system (1.1) over the rational integers $\mathbb{Z}$ as well as over the ring $\mathbb{Z}/q\mathbb{Z}$. If

$$\det \begin{pmatrix} u_1 v_1 \\ u_2 v_2 \end{pmatrix} = u_1 v_2 - u_2 v_1 \neq 0,$$

then the system has a unique solution, not necessarily integral. Otherwise, the linear space of solutions, if indeed there are any, has dimension one. Despite the relative simplicity of these 2×2 determinants, they arise in numerous arithmetic problems. We found our motivation from specific applications, for example its relevance to the problem studied in [F12]. Therein, questions arise about the summation of arithmetic functions, such as the Möbius function, over singular systems modulo q . This means that we encounter sums of the type

$$(1.2) \quad S_q = \sum_{u_1 v_2 \equiv u_2 v_1 \pmod{q}} f(u_1, v_1) g(u_2, v_2).$$

One may say we are summing over the vectors $[u_1, v_1]$ and $[v_2, -u_2]$ which are orthogonal modulo q .

For notational convenience we prefer to use arithmetic functions $c(z)$ defined on Gaussian integers $z = u + iv$; in fact the complex analytic structure of $c(z)$ will be present. Let us assume for simplicity that f, g are complex conjugate so our determinant sums are

$$(1.3) \quad S_q = \sum_{u_1 v_2 \equiv u_2 v_1 \pmod{q}} \sum_{c(z_1) \bar{c}(z_2)} c(z_1) \bar{c}(z_2) = \sum_{\text{Im } z_1 \bar{z}_2 \equiv 0 \pmod{q}} \sum c(z_1) \bar{c}(z_2).$$

Furthermore, for a technical reason, we assume that $c(z)$ is supported on odd primitive Gaussian integers $z \neq \pm 1, \pm i$, which means z has coordinates of different parity, coprime and non-zero:

$$(1.4) \quad z = u + iv, \quad u \not\equiv v \pmod{2}, \quad (u, v) = 1, \quad uv \neq 0.$$

Note that $(z, \bar{z}) = 1$.

Our main result gives a non-trivial bound for the sum of S_q over $q \leq Q$ provided $c(z)$ is supported on odd primitive numbers $1 < |z|^2 \leq X$, $|c(z)| \leq 1$, and that it satisfies a condition (of Siegel-Walfisz type) for uniformity of distribution in arithmetic progressions to small moduli. In this case we are able to prove a non-trivial bound with q running, within a few logarithms, up to X . See Section 3 for the precise statement and further remarks.

If one were to restrict z to Gaussian integers coprime with q , then the congruence $\text{Im } z_1 \bar{z}_2 \equiv 0 \pmod{q}$ could be decoupled; it is equivalent to

$$(1.5) \quad \frac{\bar{z}_1}{z_1} \equiv \frac{\bar{z}_2}{z_2} \pmod{q}.$$

This congruence can be detected by the orthogonality of characters $\psi(\bmod q)$ on the group

$$(1.6) \quad G = \{\alpha \in \mathbb{Z}[i]/q\mathbb{Z}[i] ; \alpha\bar{\alpha} \equiv 1(\bmod q)\}.$$

We obtain

$$(1.7) \quad \sum_{\substack{\operatorname{Im} z_1 \bar{z}_2 \equiv 0 (\bmod q) \\ (z_1 z_2, q) = 1}} c(z_1) \bar{c}(z_2) = \frac{1}{|G|} \sum_{\psi \in \hat{G}} \left| \sum_{(z, q) = 1} c(z) \psi(\bar{z}) / \psi(z) \right|^2.$$

Note that for q squarefree

$$(1.8) \quad |G| = \prod_{p|q} (p - \chi_4(p)),$$

while the full group of classes $\alpha(\bmod q)$, $(\alpha, q) = 1$ has larger order, namely $\varphi(q)|G|$.

Although this expression of the determinant sums in terms of characters presents quite an attractive option, we are going to work with congruences modulo q for greater transparency. Actually, this turns out to be necessary for the performance of certain transformations, such as switching moduli and enlarging moduli. These techniques, carried out here in Sections 5 and 6 respectively, are reminiscent of the strategy used previously in Sections 12 and 13 of our earlier work [F11].

The partially reduced determinant sum

$$(1.9) \quad S'_q = \sum_{\substack{u_1 v_2 \equiv u_2 v_1 (\bmod q) \\ (v_1 v_2, q) = 1}} c(z_1) \bar{c}(z_2)$$

is not very different from (1.3). Precisely, the original sum decomposes as

$$(1.10) \quad S_q = \sum_{d|q} S'_{q/d}$$

where the reduced sum $S'_{q/d}$ has coefficients $c_d(u + iw) = c(u + idw)$. The large divisors d can be easily eliminated up to negligible error terms and the small ones make an insignificant deformation of the coefficients. Now, the congruence in the reduced sum can be decoupled as

$$(1.11) \quad u_1 \bar{v}_1 \equiv u_2 \bar{v}_2 \pmod{q}$$

where $\bar{v}$ represents the multiplicative inverse of v modulo q and not complex number conjugation. Detecting (1.11) by additive characters we get

$$(1.12) \quad 0 \leq S'_q = \frac{1}{q} \sum_{a \pmod{q}} \left| \sum'_{z=u+iv} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2 \leq S_q,$$

where the latter inequality comes from positivity and the observation of the term $d = 1$ in (1.10). Here and thereafter, the stroke restricts the summation to Gaussian integers z with $(q, \text{Im } z) = 1$.

If the coefficients can be decoupled along the coordinates, say

$$(1.13) \quad c(z) = c(u + iv) = a(u)b(v),$$

then we have a more favorable expression

$$(1.14) \quad S'_q = \frac{1}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+iv \\ (v,q)=1}} a(u) \bar{b}(v) e\left(\frac{a}{q} uv\right) \right|^2.$$

To see this, open the square and change a into av_1v_2 modulo q . Here of course, $\bar{b}(v)$ does stand for the complex conjugate of $b(v)$. This expression can be treated directly by the classical large sieve inequality (consider $n = uv$ as a single variable) producing very strong estimates. Unfortunately, (1.13) does not hold in the most interesting cases and we shall need to proceed without use of this property, a task which constitutes the core of our work.

2 - A few observations about other restricted sums

When restricted to numbers $z = u + iv$ with $(uv, q) = 1$, our determinant sum modulo q , now denoted by S''_q , enjoys the symmetry

$$(2.1) \quad S''_q = \frac{1}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+iv \\ (uv,q)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2 = \frac{1}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+iv \\ (uv,q)=1}} c(z) e\left(\frac{a}{q} \bar{u} v\right) \right|^2.$$

To see this open the square and change a into $a\bar{u}_1\bar{u}_2v_1v_2$ modulo q .

The determinant sum modulo q which is restricted to numbers $z = u + iv$

with $(v, q) = 1$ and $(z, q) = 1$, denoted by S_q'''' , satisfies

$$(2.2) \quad S_q'''' = \frac{1}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+iv \\ (v,q)=(z,q)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2 \leq S_q'.$$

To see it open the square and write the congruence $\text{Im } z_1 \bar{z}_2 \equiv 0 \pmod{q}$ in the form $z_1 \bar{z}_2 \equiv \bar{z}_1 z_2 \pmod{2q}$. Hence, one of the two coprimality conditions $(z_1, q) = 1$, $(z_2, q) = 1$, is redundant and

$$(2.3) \quad S_q'''' = \frac{1}{q} \sum_{a \pmod{q}} \left(\sum'_{(z,q)=1} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right) \left(\sum'_z \bar{c}(z) e\left(-\frac{a}{q} u \bar{v}\right) \right).$$

Applying Cauchy's inequality we derive $S_q'''' \leq S_q'$.

3 - Statement of the theorem

Let $S_q(X)$ and $S_q'(X)$ denote our determinant sums modulo q with the coefficients $c(z)$ cropped to the disc

$$(3.1) \quad |z|^2 \leq X.$$

Our goal is to estimate these sums on average over $q \leq Q$, that is the sums

$$(3.2) \quad S(Q, X) = \sum_{q \leq Q} S_q(X) = \sum_{q \leq Q} \sum_{u_1 v_2 \equiv u_2 v_1 \pmod{q}} c(u_1 + i v_1) \bar{c}(u_2 + i v_2),$$

$$(3.3) \quad S'(Q, X) = \sum_{q \leq Q} S_q'(X) = \sum_{q \leq Q} \frac{1}{q} \sum_{a \pmod{q}} \left| \sum'_{\substack{z=u+iv \\ (v,q)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2.$$

Note that

$$(3.4) \quad 0 \leq S'(Q, X) \leq S(Q, X).$$

We assume that

$$(3.5) \quad |c(z)| \leq 1.$$

Then the trivial estimation of (1.3) yields

$$(3.6) \quad S(Q, X) \ll (Q + X L^5) X, \quad L = \log X,$$

and we wish to improve it by a factor of an arbitrary power of L with Q nearly as large as X . The saving factor need not be very large, yet it is crucial for applications, such as to the problem in [F12] which, as already remarked, motivated this work. But, note that the residue class $a \pmod{q}$ in (1.12) need not be reduced so in general (3.6) cannot be improved. However, it is possible to beat (3.6) if the sequence of coefficients $c(z)$ admits a considerable cancellation in sums over residue classes in the Gaussian domain to small moduli. We assume the following:

S-W condition. Let $k \geq 0$, $\ell \geq 1$, $\alpha \in \mathbb{Z}[i]$ and $t \in \mathbb{R}$. Then, we have

$$(3.7) \quad \sum_{z \equiv \alpha \pmod{\ell}} c(z) (\bar{z}/z)^k |z|^{it} \ll \ell^2 (k^2 + 1) (t^2 + 1) X L^{-B},$$

for every positive number B , with the implied constant depending only on B .

Our main example of $c(z)$ satisfying (3.7) is the Möbius function

$$(3.8) \quad c(z) = \mu(|z|^2).$$

In this case, (3.7) is just the Siegel-Walfisz condition in the Gaussian domain and we shall be using this condition for every B .

Theorem. Suppose $c(z)$ is supported on odd primitive numbers $1 < |z|^2 \leq X$, $|c(z)| \leq 1$, and that it satisfies (3.7). Then, we have

$$(3.9) \quad S(Q, X) = \sum_{q \leq Q} \sum_{u_1 v_2 \equiv u_2 v_1 \pmod{q}} c(u_1 + iv_1) \bar{c}(u_2 + iv_2) \ll (QL^{28A+148} + XL^{-A}) X,$$

for every positive number A , with the implied constant depending only on A .

4 - First estimation of $S(Q, X)$

We begin with (see (1.12))

$$(4.1) \quad S'(Q, X) = \sum_{q \leq Q} \frac{1}{q} \sum_{a \pmod{q}} \left| \sum'_{\substack{z=u+iv \\ (v,q)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2.$$

We write the fraction a/q in its lowest terms and decompose (4.1) into $T_1 + T_2$, where

$$T_1 = \sum_{\substack{qr \leq Q \\ q > Q_0}} \sum_{r} \frac{1}{qr} \sum_{a \pmod{q}}^* \left| \sum_{\substack{z=u+iv \\ (v,qr)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2$$

with Q_0 to be chosen later and T_2 is the complementary sum in which $q \leq Q_0$. We estimate T_1 by the large sieve inequality as follows:

$$\begin{aligned} T_1 &\leq \sqrt{X} \sum_v \sum_{\substack{qr \leq Q \\ q > Q_0}} \sum_{a \pmod{q}} \frac{1}{qr} \sum_{a \pmod{q}}^* \left| \sum_{z=u+iv} c(z) e\left(\frac{a}{q}u\right) \right|^2 \\ &\ll \sqrt{X} \sum_{r \leq Q} \frac{1}{r} \left(\frac{Q}{r} + \frac{\sqrt{X}}{Q_0} \right) X \ll \left(Q\sqrt{X} + \frac{X}{Q_0} \log Q \right) X. \end{aligned}$$

In the above application of the large sieve inequality the variable v does not participate and the condition $(v, qr) = 1$ has been dropped by positivity.

For estimation of T_2 we appeal to the S-W condition (3.7). To this end we generalize (3.7) as follows:

Extended S-W condition. Let $e \geq 1$, $k \geq 0$, $\ell \geq 1$, $\alpha \in \mathbb{Z}[i]$ and $t \in \mathbb{R}$. Then we have

$$(4.2) \quad \sum_{\substack{z=u+iv \equiv \alpha \pmod{\ell} \\ (v,e)=1}} c(z) (\bar{z}/z)^k |z|^{it} \ll \tau(e) \ell^2 (k^2 + 1) (t^2 + 1) X L^{-B},$$

where B is any positive number and the implied constant depends only on B .

Proof. Relax the coprimality condition $(v, e) = 1$ by the Möbius formula. Accordingly the sum (4.2) splits into

$$\sum_{d|e} \mu(d) \sum_{\substack{z=u+iv \equiv \alpha \pmod{\ell} \\ d|v}} c(z) (\bar{z}/z)^k |z|^{it}.$$

For $d \leq L^B$ apply (3.7) with ℓ replaced by $d\ell$ and B replaced by $3B$, getting the bound (4.2). For $d > L^B$ we estimate trivially by $\tau(e) X L^{-B}$. $\square$

Now we are ready to apply (4.2) for the estimation of T_2 . To this end fix u, v modulo q and apply (4.2) with $e = r$, $k = 0$, $\ell = q$ and $t = 0$. (Later, see (5.19), we shall apply it for every k and t .) The number of relevant classes $z \equiv \alpha \pmod{q}$ is q^2 , so the inner sum over z in T_2 is bounded by $\tau(r) q^4 X L^{-6B}$. Hence

$$T_2 \ll \sum_{\substack{qr \leq Q \\ q \leq Q_0}} \sum_{r} \frac{1}{qr} q \left(\tau(r) q^4 X L^{-6B} \right)^2 \ll Q_0^9 X^2 L^{4-12B}.$$

Choosing $Q_0 = L^{B+1}$ and adding the above bounds for T_1 and T_2 we conclude that

$$(4.3) \quad S'(Q, X) \ll (Q\sqrt{X} + XL^{-B})X$$

where B is any positive number and the implied constant depends only on B .

Next we use (4.3) to estimate $S(Q, X)$. We estimate $S'_{q/d}$ in (1.10) trivially by

$$\begin{aligned} \sum_{\substack{u_1 w_2 \equiv u_2 w_1 \pmod{q/d} \\ (u_1, w_1) = (u_2, w_2) = 1 \\ u_1, u_2 < \sqrt{X}; w_1, w_2 < \sqrt{X}/d}} 1 &\ll \frac{X}{d} + \sum_{1 \leq n \leq X/q} \sum_{\substack{1 \leq a, b < X/d \\ |a \pm b| = nq/d}} \tau(a)\tau(b) \\ &\ll \frac{X}{d} + \sum_{1 \leq n < X/q} \sum_{1 \leq a < X/d} \tau(a)^2 \ll \left(1 + \frac{X}{q} L^3\right) \frac{X}{d}. \end{aligned}$$

Hence

$$S(Q, X) = \sum_{q \leq Q} \sum_{\substack{d|q \\ d \leq L^C}} S'_{q/d}(X) + O((Q + XL^5)XL^{-C}),$$

where $C \geq 1$ is a constant at our disposal. This gives

$$(4.4) \quad S(Q, X) = \sum_{d \leq L^C} S'(Q/d, X) + O((Q + XL^5)XL^{-C}),$$

where the coefficients in $S'(Q/d, X)$ are $c_d(u+iv) = c(u+idv)$. These coefficients satisfy the condition (4.2) with ℓ replaced by $d\ell$; hence the upper bound (4.2) is larger by a factor $d^2 \leq L^{2C}$. This factor can be ignored because B in (4.2) is arbitrary. Therefore (4.3) applies to every $S'(Q/d, X)$ in (4.4) giving

$$S(Q, X) \ll (Q\sqrt{X}L^{2C+1} + XL^{-B})X + (Q + XL^5)XL^{-C}.$$

Hence we conclude (choose $B = A$ and $C = A + 5$):

Lemma 4.1. *For $Q \geq 1$, $X \geq 2$ we have*

$$(4.5) \quad S(Q, X) \ll \left(Q\sqrt{X}L^{2A+10} + XL^{-A}\right)X$$

where A is any positive number and the implied constant depends only on A .

Note that Lemma 4.1 yields (3.9) if $Q \leq \sqrt{X}L^{-3A-10}$.

5 - Second estimation of $S(Q, X)$

In this section we reduce the problem for larger moduli to that for smaller ones by switching divisors. For a technical reason we subdivide the range of moduli into dyadic segments. Since $S_q(X) \geq 0$ it suffices to estimate the weighted sum

$$(5.1) \quad S(\sim Q, X) = \sum_q W\left(\frac{q}{Q}\right) S_q(X)$$

where $W(x) \geq 0$ is a fixed smooth function supported on $1 < x < 4$ with $W(2) \geq 1$. Recall that

$$(5.2) \quad S_q(X) = \sum_{z_1 \bar{z}_2 \equiv \bar{z}_1 z_2 \pmod{q}} c(z_1) \bar{c}(z_2)$$

and $c(z)$ are cropped to the disc $|z|^2 \leq X$.

The determinant $z_1 \bar{z}_2 - \bar{z}_1 z_2$ vanishes only for the diagonal terms $z_1 = z_2$ which yields the contribution

$$(5.3) \quad V_0(Q, X) \ll QX.$$

On the off-diagonal we have

$$(5.4) \quad |z_1 \bar{z}_2 - \bar{z}_1 z_2| = dq \quad \text{with} \quad 1 \leq d \leq 2XQ^{-1}.$$

Let $C \geq 1$ be a constant to be specified later. If $d \leq XQ^{-1}L^{-C}$ we estimate trivially getting the contribution

$$(5.5) \quad V_1(Q, X) \ll X^2 L^{4-C}.$$

We are left with

$$(5.6) \quad V_2(Q, X) = \sum_d \sum_{z_1 \bar{z}_2 \equiv \bar{z}_1 z_2 \pmod{d}} c(z_1) \bar{c}(z_2) W(|z_1 \bar{z}_2 - \bar{z}_1 z_2|/dQ)$$

where d runs over the segment

$$(5.7) \quad DL^{-C} < d < 2D, \quad D = X/Q.$$

We need to separate the variables z_1, z_2 involved in the weight function without contaminating the coefficients $c(z_1), c(z_2)$ too much. For this job it is convenient to choose $W(x)$ in the form of the convolution

$$(5.8) \quad W(x) = \int A(x/y) B(y) y^{-1} dy$$

where $A(x)$, $B(y)$ are supported on the segments $1 \leq x, y \leq 2$. We have

$$(5.9) \quad |z_1 \bar{z}_2 - \bar{z}_1 z_2| = |z_1 z_2| |z - 1|, \quad z = z_1 \bar{z}_2 / \bar{z}_1 z_2,$$

and

$$(5.10) \quad W(|z_1 \bar{z}_2 - \bar{z}_1 z_2|/dQ) = \int A\left(\frac{2|z_1 z_2|}{dQw}\right) B\left(\frac{w}{2}|z - 1|\right) \frac{dw}{w}.$$

It follows from the support of $A(x)$ that $dQw < 2|z_1 z_2| \leq 2X$, hence $w < 2L^C$ by (5.7), and it follows from the support of $B(y)$ that $1 \leq \frac{w}{2}|z - 1| \leq w$. Therefore the variable w in the integral representation (5.10) runs over the segment

$$(5.11) \quad 1 \leq w \leq W = 2L^C.$$

Truncating the Mellin integral

$$A(x) = \int_{-\infty}^{\infty} \tilde{A}(t) x^{it} dt$$

to the segment $|t| \leq T = L^C$ and using the bound $\tilde{A}(t) \ll (t^2 + 1)^{-1}$, we obtain

$$(5.12) \quad A(x) = \int_{-T}^T \tilde{A}(t) x^{it} dt + O(T^{-1}).$$

The contribution to $V_2(Q, X)$ of the above error term is

$$(5.13) \quad V_3(Q, X) \ll X^2 L^{4-C}$$

by a trivial estimation. Hence

$$(5.14) \quad A\left(\frac{2|z_1 z_2|}{dQw}\right) = \int_{-T}^T \tilde{A}(t) \left(\frac{2|z_1 z_2|}{dQw}\right)^{it} dt + O(T^{-1}).$$

We treat $B\left(\frac{w}{2}|z - 1|\right)$ by its Fourier series expansion. Putting $z = e^{2i\alpha}$ we write

$$B\left(\frac{w}{2}|z - 1|\right) = B(w|\sin \alpha|).$$

This is an even periodic function of α of period π so we have

$$B(w|\sin \alpha|) = \sum_{k=0}^{\infty} b_k(w) \cos(2\alpha k)$$

with the coefficients

$$b_k(w) = \frac{1}{\pi} \int_0^{\pi} B(w \sin \alpha) \cos(2\alpha k) d\alpha.$$

By the support of $B(y)$ it follows that $1 < w \sin \alpha < 2$. Hence the trivial estimation yields $b_k(w) \ll w^{-1}$. If $k > 0$ we can integrate by parts two times getting

$$\begin{aligned} 4\pi k^2 b_k(w) &= - \int_0^\pi (B(w \sin \alpha))'' \cos(2\alpha k) d\alpha \\ &= -w \int_0^\pi (B'(w \sin \alpha) \cos \alpha)' \cos(2\alpha k) d\alpha. \end{aligned}$$

Hence the trivial estimation yields $b_k(w) \ll wk^{-2}$. Combining the two estimations we obtain

$$b_k(w) \ll w(k+w)^{-2}.$$

Hence

$$(5.15) \quad B\left(\frac{w}{2}|z-1|\right) = \sum_{0 \leq k < K} b_k(w) \left(z^k + z^{-k}\right) + O(wK^{-1})$$

with any $K \geq 1$. We choose $K = L^{2C}$ so the error term contributes to $V_2(Q, X)$

$$(5.16) \quad V_4(Q, X) \ll X^2 L^{4-C}$$

by a trivial estimation. We are left with

$$(5.17) \quad V_5(Q, X) = \sum_{|k| < K} \int_{-T}^T \tilde{A}(t) \left(\frac{2}{Q}\right)^{it} \nu(k, t) S^{(kt)}(D, X) dt$$

where

$$(5.18) \quad \nu(k, t) = \int_1^W b_k(w) w^{-1-it} dw \ll 1,$$

and

$$(5.19) \quad S^{(kt)}(D, X) = \sum_d \sum_{z_1 \bar{z}_2 \equiv \bar{z}_1 z_2 \pmod{d}} c(z_1) \bar{c}(z_2) |z_1 z_2|^{it} \left(\frac{\bar{z}_1}{z_1}\right)^k \left(\frac{\bar{z}_2}{z_2}\right)^{-k}.$$

Recall that $K = L^{2C}$, $T = L^C$, $W = 2L^C$ and d runs over the segment (5.7).

Our first estimation (4.5) is applicable to $S^{(kt)}(D, X)$ with Q replaced by $2D = 2XQ^{-1}$ giving

$$S^{(kt)}(D, X) \ll \left(D\sqrt{X}L^{2B+10} + XL^{-B}\right) X.$$

Hence

$$(5.20) \quad V_5(Q, X) \ll L^{3C} \left(Q^{-1} X^{\frac{3}{2}} L^{2B+10} + X L^{-B} \right) X.$$

Adding the bounds (5.3), (5.5), (5.13), (5.16) to (5.20) (with B changed into $B + 3C$, as we may since B is arbitrary), we obtain

$$S(\sim Q, X) \ll QX + X^2 L^{4-C} + L^{3C} \left(Q^{-1} X^{\frac{3}{2}} L^{2B+6C+10} + X L^{-B-3C} \right) X.$$

Now, choosing $C = B + 4$, we get

Lemma 5.1. *The weighted sum (5.1) satisfies*

$$(5.21) \quad S(\sim Q, X) \ll \left(Q + Q^{-1} X^{\frac{3}{2}} L^{11B+46} + X L^{-B} \right) X,$$

where B is any positive number and the implied constant depends only on B .

Note that, on taking $B = A + 1$, (5.21) yields

$$(5.22) \quad S(\sim Q, X) \ll (Q + X L^{-A-1}) X$$

if $Q \geq \sqrt{X} L^{12A+47}$. We still need to cover the middle range

$$(5.23) \quad \sqrt{X} L^{-3A-10} < Q < \sqrt{X} L^{12A+47}.$$

6 - Leapfrog and completing the proof

We are able to estimate the sum over this middle range of moduli by transforming it to a sum over larger moduli covered in the previous section. We accomplish this by enlarging q artificially with the aid of the primes in a segment $P < p \leq 2P$, where P is at our disposal. To simplify the notation we hide X which controls the support of $c(z)$ and so we put $S'_q = S'_q(X)$. Given a prime p , we write

$$S'_q \leq \frac{2}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+iv \\ (v,pq)=1}} c(z) e\left(\frac{a}{q} u \bar{v}\right) \right|^2 + \frac{2}{q} \sum_{a \pmod{q}} \left| \sum_{\substack{z=u+ipw \\ (w,q)=1}} c(z) e\left(\frac{a}{q} u \bar{w}\right) \right|^2.$$

Note that in the second sum we dropped the condition $(p, q) = 1$, as we can by positivity. The second sum is just the determinant sum modulo q with the coefficients $c_p(u + iw) = c(u + ipw)$, which we denote by $S_q^{(p)}$. For large p it will

be sufficient to estimate $S_q^{(p)}$ trivially. In the first sum we write $a/q = pa/pq$ and ignore that pa runs over the multiples of p , as we can by positivity. Hence the first sum is bounded by pS'_{pq} . We end up with the “enlarging moduli inequality”

$$(6.1) \quad S'_q \leq 2pS'_{pq} + 2S_q^{(p)},$$

which holds for every q and prime p .

The sum $S_q^{(p)}$ in (6.1) can be estimated trivially as follows:

$$\begin{aligned} S_q^{(p)} &\leq 4 \sum_{\substack{u_1 w_2 \equiv u_2 w_1 \pmod{q} \\ (u_1, w_1) = (u_2, w_2) = 1 \\ 1 \leq u_1, u_2 < \sqrt{X}; 1 \leq w_1, w_2 < \sqrt{X}/p}} 1 \\ &\leq \frac{4X}{p} + 8 \sum_{1 \leq n \leq X/pq} \sum_{\substack{1 \leq a, b < X/p \\ |a \pm b| = nq}} \tau(a)\tau(b) \ll \left(1 + \frac{X}{pq} L^3\right) \frac{X}{p}. \end{aligned}$$

Put

$$S'(\sim Q) = \sum_{Q < q \leq 2Q} S'_q.$$

Multiply (6.1) by $\log p$ and sum over $P < p \leq 2P$, $Q < q \leq 2Q$ getting:

Lemma 6.1. *For any $P \geq 4$ and $Q \geq 1$ we have*

$$(6.2) \quad S'(\sim Q) \ll (S'(\sim PQ) + S'(\sim 2PQ)) \log PQ + \left(Q + \frac{X}{P} L^4\right) \frac{X}{P},$$

where the implied constant is absolute.

From $S'(\sim Q)$ we go to $S(\sim Q, X)$ using the approximate formula (4.4). First, for every $S'(\sim Q/d)$ in (4.4) we apply (6.2) getting

$$\begin{aligned} S(\sim Q, X) &\ll \sum_{d \leq L^C} (S'(\sim PQ/d) + S'(\sim 2PQ/d)) \log PQ \\ &\quad + \left(QL + \frac{X}{P} L^{C+4}\right) \frac{X}{P} + (Q + XL^5) XL^{-C}. \end{aligned}$$

Now, for every $S'(\sim PQ/d)$ and $S'(\sim 2PQ/d)$ we apply (5.21) (recall that $S'(\sim Q) \leq S(\sim Q, X)$) and sum over $d \leq L^C$ getting

$$\begin{aligned} X^{-1} S(\sim Q, X) &\ll PQL^2 + (PQ)^{-1} X^{\frac{3}{2}} L^{11B+2C+47} + XL^{C-B} \\ &\quad + P^{-2} XL^{C+4} + XL^{5-C}. \end{aligned}$$

Here B, C, P are arbitrary. We take $C = A + 6$, $B = C + A + 1 = 2A + 7$, so $11B + 2C + 47 = 24A + 136$ and $P = L^{28A+147}$ getting

$$(6.3) \quad S(\sim Q, X) \ll \left(QL^{28A+147} + Q^{-1}X^{\frac{3}{2}}L^{-4A-11} + XL^{-A-1} \right) X.$$

If $Q > \sqrt{X}L^{-3A-10}$ then the middle term of (6.3) is covered by the last one. Finally, summing (6.3) over dyadic segments and incorporating (4.5) with $Q = \sqrt{X}L^{-3A-10}$, we obtain the bound (3.9). This completes the proof of the Theorem.

References

- [F11] J. B. FRIEDLANDER and H. IWANIEC, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. **148** (1998), 945–1040.
- [F12] J. B. FRIEDLANDER and H. IWANIEC, *Coordinate distribution of Gaussian primes*, J. Eur. Math. Soc. (JEMS), online first, DOI: 10.4171/JEMS/1083.

JOHN FRIEDLANDER
University of Toronto
1265 Military Trail
Toronto, ON M1C 1A4, Canada
e-mail: frdlndr@math.toronto.edu

HENRYK IWANIEC
Rutgers University
110 Frelinghuysen Rd.
Piscataway, NJ 08903, USA
e-mail: iwaniec@math.rutgers.edu